Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

г) наличие эксплуатационной документации.

Подсистема регистрации должна обеспечивать:

а) регистрацию событий в журнале аудита по следующим параметрам:

1) дата/время;

2) объект ИТ/элемент объекта ИТ;

3) результаты обработки;

б) выдачу предупреждений об обнаружении ВП;

в) генерацию отчетов.

Допускается обеспечивать выдачу предупреждений об обезвреживании ВП.».

Уточненная классификация позволит установить детальные требования для каждого типа ПСЗВВП и АПС с учетом их особенностей, что улучшит качество СЗИ допускаемых к распространению на рынке Республики Беларусь.

ПРИНЦИПЫ КЛАССИФИКАЦИИ И КЛАССИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПО УРОВНЮ РИСКА

А.В. МИСЮК, В.К. ФИСЕНКО, М.П. ТУР

Белорусский государственный университет
Объединенный институт проблем информатики НАН Беларуси

Актуальность классификации по уровню риска

Современная информационная система (ИС) – это, прежде всего, совокупность модулей, собранных в соответствии с потребностями заказчика и формируются в соответствии с иерархией системой управления владельца системы или предприятия. Основные модули ИС формируются в соответствии с иерархией системы управления предприятием.

Под классификацией ИС по уровню риска понимаем систему соподчиненных понятий областей знаний по рискам информационной безопасности или деятельности человека, используемую как средство для установления связей между этими понятиями.

Таким образом, классификация ИС по уровню рисков означает систематизацию множества ИС на основании каких-то принципов, позволяющих объединить подмножества ИС в более общие классы.

Классифицировать современные ИС достаточно сложно. Это в первую очередь связано с тем, что системы обладают модульной конструкцией и предприятие имеет возможность закупать только необходимые ему компоненты. При этом одна фирма - поставщик, как правило, выпускает модули для различных областей. Однако, в настоящее время есть достаточно вариантов классификации ИС, среди которых можно выделить классификацию ИС по разным признакам риска, в том числе по степени автоматизации (ручные, автоматизированные (по сфере применения, по характеру обработки данных), автоматические) (рис. 1), а также по уровню управления, по типу данных.

Особо следует выделить классификацию ИС по требованиям защиты информации [1]. Установлено четыре класса защищенности ИС, каждый класс которых определяется уровнем значимости информации, обрабатываемой в информационной сис-

теме. Уровень значимости информации определяется степенью возможного ущерба для обладателя информации заказчика и (или) оператора от нарушения конфиденциальности, целостности или доступности информации.

В [2] уровень риска - (degree of **risk**) представлен основным показателем, используемый для оценки отдельных рисков. Определяется как произведение вероятности возникновения риска на размер возможных финансовых потерь при наступлении рискового события.

Очевидно, что уровень риска конкретной информационной системы непосредственно связан со степенью возможного ущерба, а также с такими свойствами информационной безопасности как конфиденциальность, целостность и доступность информации. Уровень ущерба определяет возможные последствия для организации/миссии организации в случае наступления инцидента ИБ и является многокритериальной величиной (ущерб репутации, финансовый ущерб, невозможность выполнения миссии организации и т.п.). Интегрированный показатель уровня ущерба определяется по качественной шкале как максимальное значение из критериев, полученное в результате сравнения данных критериев методом анализа иерархий.

Интегрированный показатель уровня ущерба определяется по качественной шкале на основе оценок, полученных по отдельным категориям ущерба с использованием, например, метода анализа иерархий.

В рамках исследования проблемы ИБ можно выделить, например, следующие категории ущерба: от потери конфиденциальности обрабатываемой информации; от потери целостности обрабатываемой информации; от потери доступности обрабатываемой информации; от возможных сбоев и отказов оборудования; от дезорганизации деятельности организации; от нарушения и необходимости восстановления работоспособности ИС; репутационные ущербы организации.

Конфиденциальность информации: свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право.

Целостность информации: свойство безопасности информации, при котором отсутствует любое ее изменение либо изменение субъектами доступа, имеющими на него право.

Доступность информации: свойство безопасности информации, при котором субъекты доступа, имеющие права доступа, могут беспрепятственно их реализовывать.

Из изложенного следует, что:

- классификация информационных систем является задачей актуальной;

- уровень риска является функцией уровня ущерба, а также таких свойств информационной безопасности как конфиденциальность, целостность и доступность информации;

- классификация ИС по уровню риска должны базироваться на определенных принципах.

Принципы классификации информационных систем по уровню риска.

Основными принципами классификации ИС по уровню риска являются:

1) однозначность – конкретная информационная система может быть отнесена только к одной классификационной категории;

2) соответствие свойствам информационной безопасности: конфиденциальности, целостности и доступности;

3) обоснованность – используемая в формулировке классов по уровню риска степень возможного ущерба должна быть подкреплена соответствующими документами, достоверность которых может быть легко проверена;

4) динамичность – класс ИС по уроню риска может меняться на протяжении ее жизненного цикла;

5) осведомленность – собственник (владелец) ИС должен быть информирован о статусе классификации ИС;

6) прозрачность – процедуры классификации и классификационные категории четко описаны, однозначно и корректно трактуются всеми участниками;

7) идентичности продуктов и систем по свойствам безопасности (конфиденциальности, целостности и доступности) обрабатываемой информации;

8) зависимость негативных последствий от степени защищенности продуктов и систем ИТ.

Классификация информационных систем по уровню риска

В соответствии с приведенными принципами предлагается ниже приведенный вариант классификации ИС по уровню риска. На основе указанных принципов установлены следующие классы продуктов и систем ИТ по уровню риска.

Первый класс (К1) – совокупность продуктов и систем ИТ, для которых уровень риска является высоким (ущерб высокий)**,** если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия степени защищенности продуктов и систем ИТ и эти продукты и системы не могут выполнять возложенные на них функции.

Второй класс (К2) – совокупность продуктов и систем ИТ, для которых уровень риска является средним (ущерб средний), если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия степени защищенности продуктов и систем ИТ, а продукт или система не могут выполнять хотя бы одну из возложенных на них функций.

Третий класс (К3) – совокупность продуктов и систем ИТ, для которых уровень риска является низким (ущерб низкий), если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия степени защищенности продуктов и систем ИТ, а продукты и системы могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

Список литературы

1. Методический документ. Меры защиты информации в государственных информационных системах. (утв.ФСТЭК России 11.02.2014), -с.176

2. СТБ ISO/IEC 27005 – 2012. Информационные технологии. Методы обеспечения безопасности. Менеджмент рисков информационной безопасности. –с. 68